PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G07F 7/10, 7/08

A3

(11) Internationale Veröffentlichungsnummer: **WO 99/08230**

(43) Internationales Veröffentlichungsdatum: 18. Februar 1999 (18.02.99)

(21) Internationales Aktenzeichen: PCT/DE98/02147

(22) Internationales Anmeldedatum: 29. Juli 1998 (29.07.98)

(30) Prioritätsdaten:
197 34 507.7 8. August 1997 (08.08.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SEDLAK, Holger [DE/DE]; Neumünster 10A, D–85658 Egmating (DE). BRÜCKLMAYR, Franz–Josef [DE/DE]; Riedener Weg 38, D–87600 Kaufbeuren (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 29. April 1999 (29.04.99)

(54) Title: METHOD FOR VERIFYING THE AUTHENTICITY OF A DATA MEDIUM

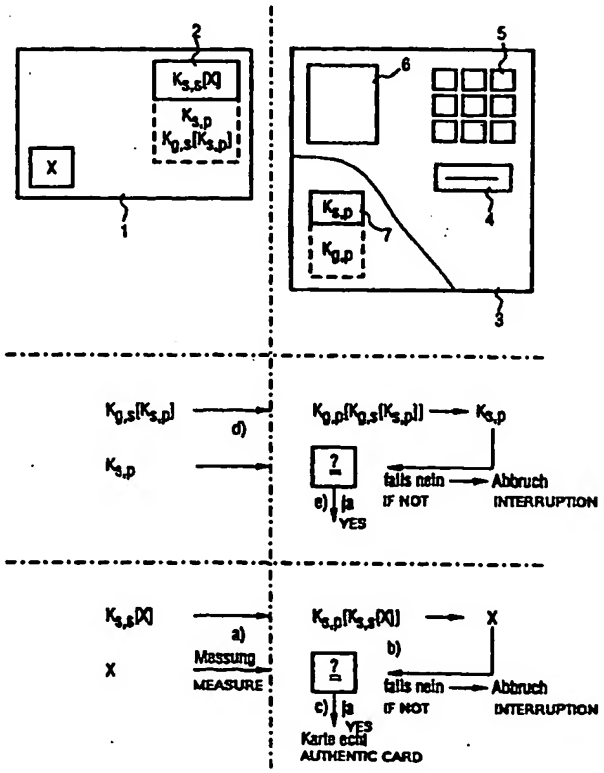
(54) Bezeichnung: VERFAHREN ZUR ECHTHEITSPRÜFUNG EINES DATENTRÄGERS

(57) Abstract

The invention concerns a method for verifying the authenticity of a data medium (1), in particular a chip card. The method is characterised in that the coded from of a physical characteristic (X) of the data medium (1) is stored in said medium. The coded form of said characteristic is transmitted to a terminal (3) which itself measures the physical characteristic (X). The latter (X) is coded with a secret code ($K_{s,s}$) and decoded with a known code ($K_{s,p}$) in the terminal (3). The authenticity is acknowledged when a coincidence is established after comparing the decoded characteristic with the measured characteristic, Said method ensures great security since the secret code ($K_{s,s}$) is contained neither in the medium (1) nor in the terminal (3).

(57) Zusammenfassung

Bei einem Verfahren zur Echtheitsprüfung eines Datenträgers (1), insbesondere einer Chipkarte, ist die verschlüsselte Form eines physikalischen Merkmals (X) des Datenträgers (1) in diesem gespeichert. Die verschlüsselte Form des Merkmals wird zu einem Terminal (3) übertragen, welches auch das physikalische Merkmal (X) selbst mißt. Das physikalische Merkmal (X) ist mit einem geheimen Schlüssel ($K_{s,s}$) verschlüsselt und wird mit einem öffentlichen Schlüssel ($K_{s,p}$) im Terminal (3) entschlüsselt. Bei einem Vergleich des entschlüsselten Merkmals und des gemessenen Merkmals wird bei Übereinstimmung die Echtheit festgestellt. Da der geheime Schlüssel ($K_{s,s}$) weder im Datenträger (1) noch im Terminal (3) enthalten ist, ist eine hohe Sicherheit gegeben.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

INTERNATIONAL SEARCH REPORT

Inten nal Application No
PCT/DE 98/02147

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0 583 709 A (THOMSON CONSUMER ELECTRONICS) 23 February 1994 see the whole document	1 2
Y	EP 0 600 646 A (PITNEY BOWES) 8 June 1994 see the whole document	2
A	GB 2 211 643 A (PITNEY BOWES) 5 July 1989 see the whole document	1,2
A	EP 0 451 024 A (GEMPLUS CARD INT) 9 October 1991 see abstract; claims; figures	1
A	DE 42 43 888 A (GAO GES AUTOMATION ORG) 30 June 1994 cited in the application see the whole document	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 March 1999	09/03/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inten nal Application No
PCT/DE 98/02147

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0583709 A	23-02-1994	CN 1082742 A,B	23-02-1994
		SG 49894 A	15-06-1998
EP 0600646 A	08-06-1994	US 5388158 A	07-02-1995
		CA 2109554 A,C	21-05-1994
		JP 7005809 A	10-01-1995
GB 2211643 A	05-07-1989	US 4853961 A	01-08-1989
		US 4893338 A	09-01-1990
		AU 2476088 A	22-06-1989
		CA 1331640 A	23-08-1994
		CH 679255 A	15-01-1992
		DE 3841393 A	29-06-1989
		FR 2625013 A	23-06-1989
		GB 2211644 A,B	05-07-1989
		JP 1191891 A	01-08-1989
		SE 468654 B	22-02-1993
		SE 8804068 A	19-06-1989
		AU 2513488 A	06-07-1989
		CA 1331641 A	23-08-1994
		CH 679346 A	31-01-1992
		DE 3841389 A	13-07-1989
		FR 2625636 A	07-07-1989
		JP 1197786 A	09-08-1989
		SE 466678 B	16-03-1992
		SE 8804236 A	23-11-1988
EP 0451024 A	09-10-1991	FR 2660465 A	04-10-1991
		CA 2039551 A	03-10-1991
		CA 2039551 C	04-10-1994
		JP 2502046 B	29-05-1996
		JP 5114060 A	07-05-1993
		US 5175424 A	29-12-1992
DE 4243888 A	30-06-1994	AT 145294 T	15-11-1996
		DE 59304496 D	19-12-1996
		WO 9415318 A	07-07-1994
		EP 0676073 A	11-10-1995
		ES 2094046 T	01-01-1997
		JP 8507164 T	30-07-1996
		SG 50470 A	20-07-1998

INTERNATIONALER RECHERCHENBERICHT

Interr. ales Aktenzeichen
PCT/DE 98/02147

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10 G07F7/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 583 709 A (THOMSON CONSUMER ELECTRONICS) 23. Februar 1994	1
Y	siehe das ganze Dokument	2
Y	EP 0 600 646 A (PITNEY BOWES) 8. Juni 1994 siehe das ganze Dokument	2
A	GB 2 211 643 A (PITNEY BOWES) 5. Juli 1989 siehe das ganze Dokument	1,2
A	EP 0 451 024 A (GEMPLUS CARD INT) 9. Oktober 1991 siehe Zusammenfassung; Ansprüche; Abbildungen	1

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. März 1999	09/03/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Interr. ...ales Aktenzeichen
PCT/DE 98/02147

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 42 43 888 A (GAO GES AUTOMATION ORG) 30. Juni 1994 in der Anmeldung erwähnt siehe das ganze Dokument	1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Intern ales Aktenzeichen
PCT/DE 98/02147

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0583709	A	23-02-1994	CN	1082742 A,B	23-02-1994
			SG	49894 A	15-06-1998
EP 0600646	A	08-06-1994	US	5388158 A	07-02-1995
			CA	2109554 A,C	21-05-1994
			JP	7005809 A	10-01-1995
GB 2211643	A	05-07-1989	US	4853961 A	01-08-1989
			US	4893338 A	09-01-1990
			AU	2476088 A	22-06-1989
			CA	1331640 A	23-08-1994
			CH	679255 A	15-01-1992
			DE	3841393 A	29-06-1989
			FR	2625013 A	23-06-1989
			GB	2211644 A,B	05-07-1989
			JP	1191891 A	01-08-1989
			SE	468654 B	22-02-1993
			SE	8804068 A	19-06-1989
			AU	2513488 A	06-07-1989
			CA	1331641 A	23-08-1994
			CH	679346 A	31-01-1992
			DE	3841389 A	13-07-1989
			FR	2625636 A	07-07-1989
			JP	1197786 A	09-08-1989
			SE	466678 B	16-03-1992
			SE	8804236 A	23-11-1988
EP 0451024	A	09-10-1991	FR	2660465 A	04-10-1991
			CA	2039551 A	03-10-1991
			CA	2039551 C	04-10-1994
			JP	2502046 B	29-05-1996
			JP	5114060 A	07-05-1993
			US	5175424 A	29-12-1992
DE 4243888	A	30-06-1994	AT	145294 T	15-11-1996
			DE	59304496 D	19-12-1996
			WO	9415318 A	07-07-1994
			EP	0676073 A	11-10-1995
			ES	2094046 T	01-01-1997
			JP	8507164 T	30-07-1996
			SG	50470 A	20-07-1998

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G06K 19/07

A2

(11) Internationale Veröffentlichungsnummer: **WO 99/08230**

(43) Internationales Veröffentlichungsdatum: 18. Februar 1999 (18.02.99)

(21) Internationales Aktenzeichen: PCT/DE98/02147

(22) Internationales Anmeldedatum: 29. Juli 1998 (29.07.98)

(30) Prioritätsdaten:
197 34 507.7 8. August 1997 (08.08.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SEDLAK, Holger [DE/DE]; Neumünster 10A, D–85658 Egmating (DE). BRÜCKLMAYR, Franz–Josef [DE/DE]; Riedener Weg 38, D–87600 Kaufbeuren (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD FOR VERIFYING THE AUTHENTICITY OF A DATA MEDIUM

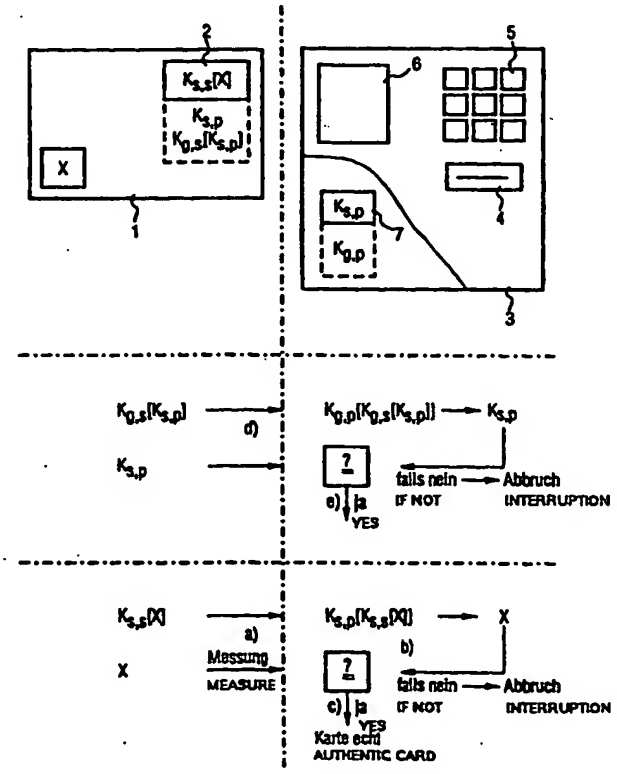
(54) Bezeichnung: VERFAHREN ZUR ECHTHEITSPRÜFUNG EINES DATENTRÄGERS

(57) Abstract

The invention concerns a method for verifying the authenticity of a data medium (1), in particular a chip card. The method is characterised in that the coded from of a physical characteristic (X) of the data medium (1) is stored in said medium. The coded form of said characteristic is transmitted to a terminal (3) which itself measures the physical characteristic (X). The latter (X) is coded with a secret code ($K_{s,s}$) and decoded with a known code ($K_{s,p}$) in the terminal (3). The authenticity is acknowledged when a coincidence is established after comparing the decoded characteristic with the measured characteristic, Said method ensures great security since the secret code ($K_{s,s}$) is contained neither in the medium (1) nor in the terminal (3).

(57) Zusammenfassung

Bei einem Verfahren zur Echtheitsprüfung eines Datenträgers (1), insbesondere einer Chipkarte, ist die verschlüsselte Form eines physikalischen Merkmals (X) des Datenträgers (1) in diesem gespeichert. Die verschlüsselte Form des Merkmals wird zu einem Terminal (3) übertragen, welches auch das physikalische Merkmal (X) selbst mißt. Das physikalische Merkmal (X) ist mit einem geheimen Schlüssel ($K_{s,s}$) verschlüsselt und wird mit einem öffentlichen Schlüssel ($K_{s,p}$) im Terminal (3) entschlüsselt. Bei einem Vergleich des entschlüsselten Merkmals und des gemessenen Merkmals wird bei Übereinstimmung die Echtheit festgestellt. Da der geheime Schlüssel ($K_{s,s}$) weder im Datenträger (1) noch im Terminal (3) enthalten ist, ist eine hohe Sicherheit gegeben.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Beschreibung

Verfahren zur Echtheitsprüfung eines Datenträgers

Die Erfindung betrifft ein Verfahren zur Echtheitsprüfung eines Datenträgers, insbesondere einer Chipkarte, der zumindest einen Speicher aufweist, wobei ein spezifisches, physikalisches Merkmal des Datenträgers in verschlüsselter Form in dem Speicher abgelegt ist.

Ein solches Verfahren ist aus der EP 0 112 461 A1 bekannt. Dort sind die Eigenschaften einer in einer Identitätskarte enthaltenen Antenne in verschlüsselter Form in der Karte gespeichert und werden mit den gemessenen Eigenschaften verglichen. Der Vergleich findet dort jedoch in der Karte statt, wobei das wesentliche Geheimnis der Verschlüsselungsalgorithmus ist.

Datenträger, die einem Echtheitsprüfungsverfahren unterzogen werden sollen, weisen meist einen Zähler auf, dessen Stand einen Geldwert repräsentiert und liefern daher einen Kopier- bzw. Nachbauanreiz. Aber auch bei der Verwendung solcher Datenträger bei Zutrittskontrollsystemen oder im Bereich der Sozialversicherungen ist ein solcher Anreiz gegeben.

Es ist möglich, einen Halbleiterchip identisch zu kopieren, so daß auch alle Geheimzahlen und verschlüsselten Daten wie das verschlüsselte physikalische Merkmal auf der Kopie enthalten sind, ohne den genauen Schaltungsaufbau verstanden zu haben, so daß hier ein großes Sicherheitsrisiko vorliegt. Die Durchführung einer Echtheitsprüfung mittels eines physikalischen Merkmals, das bei jedem Datenträger anders und möglichst kompliziert ist und somit sehr schwer nachzubauen ist, ist jedoch ein erster Schritt zu einer höheren Fälschungssicherheit, da ein Betrüger zwar einen Chip nachbauen kann aber

kaum eine dazu passende Karte mit dem richtigen physikalischen Merkmal.

Das bekannte Verfahren bringt hier allerdings noch keine zufriedenstellende Fälschungssicherheit. Da der Vergleich in der Karte bzw. im in der Karte enthaltenen Halbleiterchip stattfindet, ist es möglich, einen Chip oder eine Karte nachzubauen, der oder die immer ein positives Vergleichsergebnis an das Terminal meldet, unabhängig von einem tatsächlich durchgeführten Vergleich. Würde der Vergleich bei dem bekannten Verfahren jedoch im Terminal stattfinden, müßte in jedem Terminal der Verschlüsselungsalgorithmus sowie die geheim zu haltende Schlüsselzahl vorhanden sein, um entweder die gemessenen Daten ebenfalls zu verschlüsseln und die verschlüsselten Formen zu vergleichen oder die aus der Karte ausgelesene verschlüsselte Form der Daten zu entschlüsseln und die Originaldaten zu vergleichen. Dies birgt jedoch erhebliche Sicherheitsrisiken, da es einem Betrüger Anreize bietet, Terminals zu entwenden und zu analysieren.

Das der Erfindung zugrunde liegende Problem ist also, ein Verfahren zur Echtheitsprüfung von Datenträgern anzugeben, das ein hohes Maß an Sicherheit bietet und die oben genannten Nachteile vermeidet.

Das Problem wird durch ein Verfahren gemäß Anspruch 1 gelöst. Eine vorteilhafte Weiterbildung ist im Unteranspruch angegeben.

Beim erfindungsgemäßen Verfahren wird der Vergleich im Terminal durchgeführt, ohne daß der geheime Schlüssel im Terminal vorhanden sein muß, da eine asymmetrische Verschlüsselung verwendet wird. Asymmetrische Verschlüsselung bedeutet, daß zum Verschlüsseln ein anderer Schlüssel verwendet wird als zum Entschlüsseln und selbst bei Kenntnis des jeweils anderen keiner der beiden Schlüssel berechnet werden kann. Der Entschlüsselungsschlüssel kann allgemein bekannt sein und wird

in der Regel jedermann zugänglichen Dateien - beispielsweise aus dem Internet - entnehmbar sein.

Der öffentliche Schlüssel ist hierbei einem bestimmten speziellen Kartensystembetreiber, wie Kreditkartengesellschaften oder Banken und Versicherungen zugeordnet. Wesentlich beim erfindungsgemäßen Verfahren ist, daß der geheime, nur dem Systembetreiber bekannte Schlüssel nicht aus dem öffentlichen Schlüssel berechnet werden kann. Als Beispiel für ein asymmetrisches Verschlüsselungsverfahren wird das RSA-Verfahren genannt.

Wenn lediglich das verschlüsselte Merkmal zum Terminal übertragen wird, ist es nötig, daß im Terminal die öffentlichen Schlüssel sämtlicher Systembetreiber gespeichert oder über beispielsweise einen Intranetanschluß zugreifbar sind, die sich dieses Terminals bedienen wollen. Um diesen Nachteil zu vermeiden, ist in Weiterbildung der Erfindung der öffentliche, spezielle Schlüssel in verschlüsselter Form in der Karte abgespeichert, wobei zu dessen Verschlüsselung ein geheimer, globaler Schlüssel verwendet wurde. Dieser geheime, globale Schlüssel ist beispielsweise nur Zentralbanken oder sonstigen hoheitlichen Institutionen bekannt. Er wird für die Verschlüsselung jedes öffentlichen, speziellen Schlüssels verwendet. In der Karte ist außerdem der unverschlüsselte, öffentliche, spezielle Schlüssel gespeichert.

Im Terminal ist dann lediglich der zum geheimen, globalen Schlüssel gehörende öffentliche, globale Schlüssel enthalten, mittels dem die verschlüsselte Form des öffentlichen, speziellen Schlüssels entschlüsselt und mit dem Originalschlüssel, der ja ebenfalls gespeichert ist, verglichen wird. Eine Übereinstimmung zeigt dann, daß zum Verschlüsseln des öffentlichen, speziellen Schlüssels der richtige geheime, globale Schlüssel verwendet wurde und bedeutet eine Zertifizierung beispielsweise der Zentralbank, die somit dafür bürgt, daß

der öffentliche, spezielle Schlüssel korrekt ist und zum Entschlüsseln des physikalischen Merkmals verwendet werden kann.

Als physikalisches Merkmal kann bei kontaktlosen Datenträgern eine Antenneneigenschaft wie beispielsweise die Güte oder auch Kombinationen solcher Eigenschaften verwendet werden. Weitere Möglichkeiten für physikalische Merkmale sind in der EP 0 676 073 B1 und der EP 0 602 643 A2 angegeben. Dort werden ein einstellbares Widerstandsnetzwerk bzw. die Eigenschaften einer EEPROM-Zelle als kartenspezifisches, physikalisches Merkmal vorgeschlagen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe einer Figur näher beschrieben. Die Figur zeigt dabei in schematischer Weise eine Chipkarte und ein Lese/Schreib-Terminal sowie ein Ablaufdiagramm des erfindungsgemäßen Verfahrens.

Die Figur zeigt eine Chipkarte 1, die einen Speicher 2, der beispielsweise in einem Halbleiterchip realisiert sein kann, sowie ein physikalisches Merkmal X aufweist.

Trotz der Darstellung einer Chipkarte ist die Erfindung keineswegs auf eine solche Ausgestaltung eingeschränkt, sondern kann bei beliebigen Formen von Datenträgern angewendet werden.

Im Speicher 2 ist zumindest die mit einem ersten geheimen, speziellen Schlüssel K_{ss} verschlüsselte Form $K_{s,s}[X]$ des Merkmals X enthalten. Wie durch eine strichliert dargestellte Vergrößerung des Speichers 2 angedeutet ist, kann in Weiterbildung der Erfindung außerdem ein zweiter öffentlicher, spezieller Schlüssel $K_{s,p}$ sowie die verschlüsselte Form dieses zweiten Schlüssels $K_{g,s}[K_{s,p}]$ enthalten sein. Zum Verschlüsseln des zweiten Schlüssels $K_{s,p}$ wurde ein dritter geheimer, globaler Schlüssel $K_{g,s}$ verwendet.

Durch eine senkrechte, strichlierte Linie von der Chipkarte 1 getrennt ist ein Terminal 3 dargestellt. Dieses weist einen Aufnahmeschacht 4 für die Chipkarte 1 auf sowie eine Tastatur 5 und ein Display 6. Das Terminal 3 weist außerdem einen Speicher 7 auf, in dem wenigstens temporär der zweite öffentliche, spezielle Schlüssel $K_{s,p}$ gespeichert ist. Das Terminal 3 kann diesen Schlüssel einerseits permanent gespeichert haben, aber auch für jede Echtheitsprüfung über einen Datenleitung von einer Zentrale oder aus einem Datennetz holen. Da es sich bei dem zweiten Schlüssel $K_{s,p}$ um einen speziellen Schlüssel handelt, der einem bestimmten Systembetreiber, wie beispielsweise einer Kreditkartenfirma zugeordnet ist, das Terminal 3 jedoch möglicherweise für Karten unterschiedlicher Systembetreiber anwendbar sein soll, wäre es nötig, verschiedene zweite öffentliche, spezielle Schlüssel gespeichert zu halten. Stattdessen kann in Weiterbildung der Erfindung ein vierter öffentlicher, globaler Schlüssel $K_{g,p}$ gespeichert sein, was durch eine strichlierte Erweiterung des Speichers 7 angedeutet ist.

Sowohl die Chipkarte 1 als auch das Terminal 3 können weitere Einrichtungen, wie Mikroprozessoren oder Kryptoprozessoren enthalten. Die Übertragung von der Chipkarte 1 zum Terminal 3 kann sowohl in kontaktbehafter Weise als auch kontaktlos, beispielsweise über induktive Kopplung erfolgen. Das Terminal 3 weist außerdem eine Meßeinrichtung auf, um das physikalische Merkmal X der Chipkarte 1 ermitteln zu können. All diese Details sind nicht in der Figur dargestellt, da sie bereits aus dem Stand der Technik bekannt sind und im Detail nicht zur Erfindung beitragen.

In der Figur ist unter der Darstellung der Chipkarte 1 und des Terminals 3 der Ablauf des erfindungsgemäßen Verfahrens dargestellt. Zwischen horizontalen strichlierten Linien ist die Weiterbildung der Erfindung dargestellt, falls im Terminal 3 lediglich ein öffentlicher, globaler Schlüssel enthalten ist. In diesem Fall wird in einem Verfahrensschritt d)

die verschlüsselte Form des öffentlichen, speziellen Schlüssels sowie der öffentliche, spezielle Schlüssel selbst von der Chipkarte 1 zum Terminal 3 übertragen, im Terminal 3 mittels des öffentlichen, globalen Schlüssels der öffentliche, spezielle Schlüssel berechnet und mit dem übertragenen öffentlichen, speziellen Schlüssel im Verfahrensschritt e) verglichen. Falls keine Übereinstimmung gegeben ist erfolgt ein Abbruch des Verfahrens.

Bei Übereinstimmung wird im Verfahrenschritt a) die verschlüsselte Form des physikalischen Merkmals von der Chipkarte 1 zum Terminal 3 übertragen sowie das physikalische Merkmal selbst vom Terminal 3 gemessen. Im Terminal wird dann mittels des zuvor übertragenen und als richtig erkannten öffentlichen, speziellen Schlüssels $K_{s,p}$ das verschlüsselte physikalische Merkmal entschlüsselt und mit dem gemessenen verglichen.

Falls eine Übereinstimmung ergeben ist, wird die Karte im Verfahrensschritt c) als echt erkannt. Falls keine Übereinstimmung gegeben ist, erfolgt ein Abbruch des Verfahrens.

Bei Anwendung des erfindungsgemäßen Verfahrens brauchen in der Chipkarte 1 lediglich die verschlüsselten Formen des Merkmals X sowie des öffentlichen, speziellen Schlüssels und der öffentliche, spezielle Schlüssel selbst gespeichert sein. Der geheime, spezielle und der geheime, globale Schlüssel brauchen in der Chipkarte 1 nicht vorhanden zu sein, sondern müssen lediglich dem Systembetreiber bzw. der zertifizierenden Stelle bekannt sein. Da die geheimen Schlüssel jedoch eindeutig den zugehörigen öffentlichen Schlüsseln zugeordnet sind, ist es nicht möglich, eine Karte nachzubauen, die die korrekten verschlüsselten Formen der zur Echtheitsprüfung benötigten Daten enthalten.

Auch eine Entwendung und Analyse eines Terminals 3 seitens eines Betrügers führt nicht zum gewünschten Erfolg, da auch

dort lediglich die öffentlichen und somit auch andersweitig erhaltbaren Schlüssel gespeichert sind. Sowohl im Datenträger als auch im Terminal können die geheimen, speziellen und der geheime, globale Schlüssel enthalten sein, obwohl dies nicht nötig ist, allerdings würde dies zu einem Sicherheitsverlust führen.

Patentansprüche

1. Verfahren zur Echtheitsprüfung eines Datenträgers (1), insbesondere einer Chipkarte,
der zumindest einen Speicher (2) aufweist, wobei ein spezifisches, physikalisches Merkmal (X) des Datenträgers (1) in verschlüsselter Form ($K_{s,s}[X]$) in dem Speicher (2) abgelegt ist,
dadurch gekennzeichnet,
daß das Merkmal (X) mit einem ersten geheimen, speziellen Schlüssel ($K_{s,s}$) verschlüsselt ist,
daß ein zum ersten geheimen Schlüssel ($K_{s,s}$) gehörender zweiter spezieller, öffentlicher Schlüssel ($K_{s,p}$) in einem Lese/Schreib-Terminal (3) vorhanden ist,
daß die folgenden Schritte ausgeführt werden:
a) das Lese/Schreib-Terminal (3) liest das verschlüsselte Merkmal ($K_{s,s}[X]$) aus dem Speicher (2) des Datenträgers (1) und ermittelt das physikalische Merkmal (X) durch Messung,
b) das Lese/Schreib-Terminal (3) errechnet mit dem zweiten Schlüssel ($K_{s,p}$) das Merkmal ($X=K_{s,p}[K_{s,s}[X]]$) und vergleicht es mit dem gemessenen Merkmal (X)
c) bei Übereinstimmung wird die Echtheit des Datenträgers (1) festgestellt.

2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet,
daß im Datenträger (1) zusätzlich der zweite spezielle, öffentliche Schlüssel ($K_{s,p}$) und die mit einem dritten globalen, geheimen Schlüssel ($K_{g,s}$) verschlüsselte Form des zweiten Schlüssels ($K_{g,s}[K_{s,p}]$) gespeichert ist,
daß folgende Schritte ausgeführt werden
d) das Terminal (3) liest diese Daten und errechnet mit einem im Terminal (3) vorhandenen vierten globalen, öffentlichen Schlüssel ($K_{g,p}$) den zweiten Schlüssel ($K_{s,p}=K_{g,p}[K_{g,s}[K_{s,p}]]$) und vergleicht diesen mit dem gelesenen zweiten Schlüssel,
e) bei Übereinstimmung werden die Verfahrensschritte a) bis c) ausgeführt.

1/1